[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 15/163
G06F 15/173

[12]发明专利申请公开说明书

[21]申请号 00123517.6

[43]公开日 2002年3月13日

[11]公开号 CN 1339749A

[22]申请日 2000.8.18 [21]申请号 00123517.6

[71]申请人 清华大学
地址 100084 北京市海淀区清华大学
共同申请人 富士通株式会社
[72]发明人 牛志升

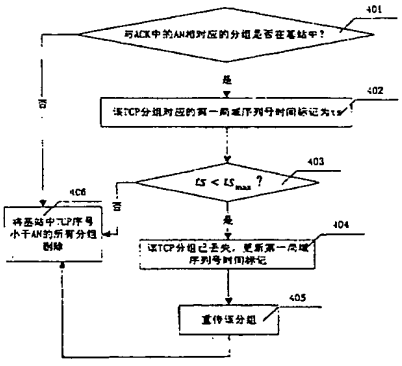
[74]专利代理机构 北京三友知识产权代理有限公司
代理人 韩飘扬 宋志强

权利要求书4页 说明书11页 附图页数2页

[54]发明名称 一种将TCP用于不可靠传输网络的局域重传方法

[57]摘要

本发明涉及一种将传输控制协议(TCP)用于不可靠传输网络的局域重传 方法,可在不可靠传输链路上对乱序的TCP分组数据提供可靠传递,对所有非 拥塞丢失的分组进行恢复,避免TCP源端不真实的窗口容量调整。采用链路层 传输顺序与TCP源端的发送顺序一起检测的TCP局域重传方法,通过在TCP数 据分组与TCP确认分组中插入局域序列号时间标记,并与确认序号AN联合判 断,来确定是否有数据分组丢失并重传,然后再采用明晰重传ERN反馈来避免TCP源端的误动作。可大大改善无线网络的TCP性能。



ISSN1008-4274

00.08.10

权 利 要 求 书

1. 一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于包括以下步骤：

A. 不可靠链路接入点每接收到一个来自国际互联网络上 TCP 源端的新的 TCP 数据分组，则在该数据分组头插入一个包含有第一局域序列号时间标记的 LAC－PDU 头，即将该数据分组封装成“LAC－PDU 头＋IP 头＋TCP 头＋数据”的 LAC－PDU 数据分组向当前终端发送；

B. 当前终端对成功接收的 TCP 数据分组产生一个包含确认序号（AN）的确认（ACK1）分组，在该确认分组头也插入一个包含有第二局域序列号时间标记的 LAC－PDU 头，即将该确认分组封装成 LAC－PDU 确认分组反馈发送至不可靠链路接入点；

C. 不可靠链路接入点根据接收到的确认分组中的确认序号（AN）、第二局域序列号时间标记和存储在不可靠链路接入点的第一局域序列号时间标记作判断，当判断出有丢失的数据分组时，按步骤 A 的方法更新其 LAC－PDU 头的第一局域序列号时间标记并重传该数据分组，在判断确认分组（ACK1）中的确认序号（AN）所对应的数据分组不可能发生拥塞丢失时，则标记该确认分组（ACK1）中的明晰重传反馈（ERN）域，并发送至 TCP 源端。

2. 根据权利要求 1 所述的一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于：所述的步骤 A 中，在数据分组头插入一个包含有第一局域序列号时间标记的 LAC－PDU 头时，还同时将该封装好的 LAC－PDU 数据分组的副本存入一缓冲器中。

3. 根据权利要求 1 或 2 所述的一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于：所述的第一局域序列号时间标记是具有固定比特长度的域，随实际发送数据分组数的增加，从零开始以 1 为步长顺序记录。

4. 根据权利要求 1 或 2 所述的一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于：所述的在从不可靠链路接入点到终端的发送全过程中，其

实际发送顺序是由各 TCP 数据分组中对应的第一局域序列号时间标记值唯一确定的。

5. 根据权利要求 1 或 2 所述的一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于：所述的第二局域序列号时间标记也是具有固定比特长度的域，域中记录的是当前终端所接收到的所有成功传送的 TCP 数据分组中所携带的第一局域序列号时间标记中的最大值。

6. 根据权利要求 1 或 2 所述的一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于：所述的不可靠链路接入点根据接收到的确认分组中的确认序号（AN）、第二局域序列号时间标记，和存储在不可靠链路接入点的第一局域序列号时间标记作判断，判断出有丢失的数据分组，进一步包括：判断确认分组中与确认序号（AN）相对应的数据分组是否还在不可靠链路接入点中；若还在，则将该数据分组中对应的第一局域序列号时间标记与确认分组中的第二局域序列号时间标记作大小比较；若第一局域序列号时间标记小于第二局域序列号时间标记，则判断该数据分组丢失，更新该数据分组中 LAC－PDU 头中的第一局域序列号时间标记并重传该数据分组；另外，将不可靠链路接入点中所有 TCP 序列号小于确认序号（AN）的数据分组删除。

7. 根据权利要求 6 所述的一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于：所述的在更新该数据分组中 LAC－PDU 头中的第一局域序列号时间标记并重传该数据分组时，是将该数据分组中的第一局域序列号时间标记表示为当前的传送顺序后再重传。

8. 根据权利要求 6 所述的一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于：所述的将不可靠链路接入点中所有 TCP 序列号小于确认序号（AN）的数据分组删除，包括：在判断确认分组中与确认序号（AN）相对应的数据分组不在不可靠链路接入点中时：在第一局域序列号时间标记大于或等于第二局域序列号时间标记时；和在判断数据分组丢失，于更新并重传该数据分组后。

00.09.18

9 根据权利要求 6 所述的一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于：所述的确认分组头中的明晰重传（ERN）反馈是一位比特，在不可靠链路接入点判断出与确认序号（AN）相对应的数据分组在不可靠链路接入点中时，将发送至 TCP 源端的确认分组（ACK1）的该明晰重传（ERN）反馈比特置为 1；TCP 源端在收到明晰重传（ERN）反馈比特为 1 的确认分组（ACK1）后，若与该确认分组（ACK1）相对应的 TCP 数据分组发生快速重传或超时重传时，仅重发该数据分组，但不作任何减小发送窗口的操作。

10 根据权利要求 1 所述的一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于：所述的第一局域序列号时间标记或第二局域序列号时间标记的长度是不可靠链路接入点所能容纳的 TCP 连接的最大分组数。

11 根据权利要求 1 所述的一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于：所述的第一局域序列号时间标记或第二局域序列号时间标记的长度是 8 个比特，其中包括一个用于溢出控制的进位比特。

12. 根据权利要求 1 所述的一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于：所述步骤 A 中 LAC－PDU 数据分组头中的第一局域序列号时间标记也可以用底层传输序号代替，再建立 TCP 数据分组的序列号与该底层传输序号间的对应关系；所述步骤 B 中的第二局域序列号时间标记是终端成功接收的最大底层传输序号。

13. 一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于：是用于移动通信系统传送数据分组的方法，该系统接收来自国际互联网的包含序列号的数据分组，并将该分组发往移动终端，所述的传送方法包括如下步骤：

接收来自国际互联网的数据分组；

将第一局域序列号时间标记赋予每个接收到的数据分组；

按移动通信系统使用的格式形成带有第一局域序列号时间标记的分组数据；

存储该带有时间标记的分组数据；

将所形成的分组数据发送到移动终端;

当移动终端成功地接收到所发送的分组数据时，移动终端回发确认数据，该确认数据包括确认序号和相应于所接收的第一局域序列号时间标记的第二局域序列号时间标记;

通过将存储的序列号和第一序列号时间标记与发回的确认数据进行比较，确定应向移动终端重传的数据分组;

重传所确定的数据分组。

14. 根据权利要求 13 所述的一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于：所述的传送数据分组的方法中，所述的移动通信系统包括一个服务器，所述的服务器将第一局域序列号时间标记赋予每个接收到的数据分组，并按移动通信系统使用的格式形成带有第一局域序列号时间标记的分组数据，和存储该带有时间标记的分组数据。

15. 一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于：是接收移动通信系统中移动终端数据分组的方法，该系统接收来自国际互联网的包含序列号的数据分组，并将该分组发往移动终端；所述的接收方法包括以下步骤:

接收一个新的数据分组，该数据分组按移动通信系统使用的格式形成，所形成的数据分组包括第一局域序列号时间标记;

相应于所接收到的第一局域序列号时间标记给出第二局域序列号时间标记;

回发确认数据，该确认数据包括确认序列号和相应于所接收到的第一局域序列号时间标记给定的第二局域序列号时间标记。

说　明　书

一种将 TCP 用于不可靠传输网络的局域重传方法

本发明涉及一种不可靠网络的重传方法，更确切地说是涉及一种认知传输控制协议（TCP－Transport Control Protocol）的局域重传方法（TCP Aware Local Retransmission），该方法可在不可靠传输链路上提供可靠的重传，并可有效地避免不同层协议间的不利干扰，从而大大改善不可靠网络的 TCP 性能。

随着国际互联网（因特网）的迅速发展，使其很可能成为未来多媒体网络的统一平台，因此，利用各种网络技术接入国际互联网就显得十分重要，其中，通过移动通信系统接入国际互联网则尤为现实。目前，国际电讯联盟（ITU）正致力于制定第三代移动通信系统（IMT2000）的国际标准，预计，该移动通信系统就能支持互联网上多变的计算和随机的接入（nomadic access）。可以说，随着网络技术的不断发展以及商业需求的不断扩展，因特网所依托的底层网络特性也将会呈现出多样化的发展趋势。令因特网创建者始料未及的是创建之初对网络特性的简单假设，使因特网的许多核心协议不能适应未来多样性的混合网络，这一点在 TCP 上体现得尤其明显。

TCP 原是为有线网络设计的，目前该协议已广泛用于互联网，为国际互联网上提供可靠传输业务，如 WWW 浏览、远程登录（Telnet）、文件传输（FTP）等的核心协议。然而该协议赖以实现的许多基础技术在目前看来是不可靠的，例如，TCP 将所有的分组(packet)丢失(loss)都判为是拥塞(congestion)造成的。

一般说来，TCP 性能是由拥塞控制和差错恢复两种技术手段来保证的，其中 TCP 性能的拥塞控制是基于滑动窗口机制，该机制经过反复的改进，目前已近完美。差错恢复的核心思想是确认反馈，通过有限的反馈信息传递，即由 ACK（acknowledge）、NACK （non－acknowledge）来获得是否重传的相关信息，但其本身不能很好地解决拥塞丢失与非拥塞丢失的区别问题，即，不管是拥塞

丢失还是非拥塞丢失， TCP 源端只要收到 ACK 则自动提升窗口尺寸，只要收到 NACK 则自动降低窗口尺寸，将发送窗口的尺寸自动调整到网络的容量（吞吐量），以减少发生拥塞的机会。而在实际传输过程中，特别是在不可靠网络如无线传输链路中，由于无线环境下误码率较高，在恶劣信道中的非拥塞丢失现象比较严重，因而错误地触发拥塞控制，造成不真实的窗口尺寸调整，使网络资源的利用率降低，同时也因发送窗口的剧烈震荡，导致 TCP 性能恶化。因此，TCP 在不可靠网络如无线网络中使用还面临许多实际问题。

另一方面，TCP 对于丢失分组的恢复能力也十分有限，为此，提出了许多提高分组重传速度与效率的改进性建议，诸如，TCP-New Reno（参考文献[1]J. C. Hoe. Improving the Start-Up Behavior of a Congestion Control Scheme for TCP. In proc. ACM SIGCOMM 96, August 1996)和 TCP-SACK(参考文献[2]K. Fall and S. Floyd. Simulation-based Comparisons of Tahoe, Reno and Sack TCP. Computer Communication Review, July 1996.)。但所有这些改进建议都没有解决对丢失原因的正确解析这一难题，如果利用明晰反馈 ELN（Explicit Loss Notification，参考文献[3] Hari, Balakrishnan , Randy H. Katz, Explicit Loss Notification and Wireless Web Performance , Globecom 98, Sydney , Australia , Novermber 1998.）比特来解决，又需要对国际互联网的核心协议作修改，故没有可行性。

综上所述，总的说来在混合网络特别是在有无线网络的混合网络中，急待要解决的问题就是区分分组的拥塞丢失与非拥塞丢失，以及针对非拥塞丢失时的不真实的窗口尺寸调整。

为解决这些问题，提出了一些本地解决办法，诸如基于链路层协议的航空邮件（AIRMAIL，参考文献[4] E. Ayanoglu, S. Paul, T. F. Laporta, K. K. Sabnani, and R. D. Gitlin. AIRMAIL: A Link-Layer protocol for Wireless Network. ACM ACM/Baltzer Wireless Networks Journal , 1: 47-60, February 1995.）和其它的自动重发请求/前向纠错

(ARQ/FEC-automatic retransmission request/forward error correction)。它们通过重传丢失的分组来改善 TCP 的性能，但是，若采用这些纯本地的解决办法，为了可靠传输需要增加大量的附加负荷，因此而降低了效率。在参考文献 Snoop[5] (H. Balakrishnan, S, Seshan, and R. H. Katz. Improving Reliable Transport and Handoff Performance in Cellular Wireless Networks, ACM Wireless Networks , (December 1995)中引入的 TCP 认知(awareness)概念，就是为解决这一问题的，该概念通过在链路层使用 TCP/ACK (传输控制协议/确认)分组来提供本地的重传，由于仍然使用定时器来恢复乱序的丢失分组，这就要求对无线链路的环路时间进行精确的估算；此外，在基站中设置定时器将要浪费相当大的系统资源；还有，阻止复制 ACK 的方法不可能完全避免 TCP 源端的不必要的超时。

拥塞或重传都能导致乱序传递。如果，一乱序分组在无线链路中丢失，它不可能通过使用重复的 ACK 或部分的 ACK 来恢复，因此，流行的解决办法之一就是使用超时重传，然而这就要求精确地估算出无线链路的环路时间，这在本身就不可靠的无线网络中是难于做到的。

该问题的另一解决办法是使用一种纯粹的链路层协议，诸如自动重发请求(ARQ)，由协议给每个分组一个新的序号，以便标识出分组到达的顺序并利用它来恢复丢失，但其额外的开销又可能造成低效率问题。

本发明的目的是设计一种将 TCP 用于不可靠传输网络的局域重传方法，以有效解决乱序分组的丢失，和通过区别拥塞丢失与非拥塞丢失避免 TCP 源端的误动作，以提高不可靠传输链路上的 TCP 性能。

本发明的方法是传输层与链路层共同作用的技术方案，也就是通过将链路层传输顺序与 TCP 源端的发送顺序一起检测的 TCP 认知局域重传 (TCP - Aware Local Retransmission)，来确定是否有数据分组丢失，然后再采用明晰重传 (ERN - Explicit Retransmission Notification) 反馈来避免 TCP 源端的误动作。本发明的方案是基于 TCP 认知局域(本地)重传上的。

本发明的目的是这样实现的：一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于包括以下步骤：

A. 不可靠链路接入点每接收到一个来自国际互联网络上 TCP 源端的新的 TCP 数据分组，则在该数据分组头插入一个包含有第一局域序列号时间标记的 LAC－PDU 头，即将该数据分组封装成“LAC－PDU 头＋IP 头＋TCP 头＋数据”的 LAC－PDU 数据分组向当前终端发送；

B. 当前终端对成功接收的 TCP 数据分组产生一个包含确认序号（AN）的确认（ACK1）分组，在该确认分组头也插入一个包含有第二局域序列号时间标记的 LAC－PDU 头，即将该确认分组封装成 LAC－PDU 确认分组反馈发送至不可靠链路接入点；

C. 不可靠链路接入点根据接收到的确认分组中的确认序号（AN）、第二局域序列号时间标记和存储在不可靠链路接入点的第一局域序列号时间标记作判断，当判断出有丢失的数据分组时，按步骤 A 的方法更新其 LAC－PDU 头的第一局域序列号时间标记并重传该数据分组，在判断确认分组（ACK1）中的确认序号（AN）所对应的数据分组不可能发生拥塞丢失时，则标记该确认分组（ACK1）中的明晰重传反馈（ERN）域，并发送至 TCP 源端。

所述的步骤 A 中，在数据分组头插入一个包含有第一局域序列号时间标记的 LAC－PDU 头时，还同时将该封装好的 LAC－PDU 数据分组的副本存入一缓冲器中。

所述的第一局域序列号时间标记是具有固定比特长度的域，随实际发送数据分组数的增加，从零开始以 1 为步长顺序记录。

所述的在从不可靠链路接入点到终端的发送全过程中，其实际发送顺序是由各 TCP 数据分组中对应的第一局域序列号时间标记值唯一确定的。

所述的第二局域序列号时间标记也是具有固定比特长度的域，域中记录的是当前终端所接收到的所有成功传送的 TCP 数据分组中所携带的第一局域序列号时间标记中的最大值。

所述的不可靠链路接入点根据接收到的确认分组中的确认序号（AN）、第二局域序列号时间标记，和存储在不可靠链路接入点的第一局域序列号时间标记作判断，判断出有丢失的数据分组，进一步包括：判断确认分组中与确认序号（AN）相对应的数据分组是否还在不可靠链路接入点中；若还在，则将该数据分组中对应的第一局域序列号时间标记与确认分组中的第二局域序列号时间标记作大小比较；若第一局域序列号时间标记小于第二局域序列号时间标记，则判断该数据分组丢失，更新该数据分组中 LAC－PDU 头中的第一局域序列号时间标记并重传该数据分组；另外，将不可靠链路接入点中所有 TCP 序列号小于确认序号（AN）的数据分组删除。

所述的在更新该数据分组中 LAC－PDU 头中的第一局域序列号时间标记并重传该数据分组时，是将该数据分组中的第一局域序列号时间标记表示为当前的传送顺序后再重传。

所述的将不可靠链路接入点中所有 TCP 序列号小于确认序号（AN）的数据分组删除，包括：在判断确认分组中与确认序号（AN）相对应的数据分组不在不可靠链路接入点中时：在第一局域序列号时间标记大于或等于第二局域序列号时间标记时；和在判断数据分组丢失，于更新并重传该数据分组后。

所述的确认分组头中的明晰重传（ERN）反馈是一位比特，在不可靠链路接入点判断出与确认序号（AN）相对应的数据分组在不可靠链路接入点中时，将发送至 TCP 源端的确认分组（ACK1）的该明晰重传（ERN）反馈比特置为 1；TCP 源端在收到明晰重传（ERN）反馈比特为 1 的确认分组（ACK1）后，若与该确认分组（ACK1）相对应的 TCP 数据分组发生快速重传或超时重传时，仅重发该数据分组，但不作任何减小发送窗口的操作。

所述的第一局域序列号时间标记或第二局域序列号时间标记的长度是不可靠链路接入点所能容纳的 TCP 连接的最大分组数。

所述的第一局域序列号时间标记或第二局域序列号时间标记的长度是 8 个比特，其中包括一个用于溢出控制的进位比特。

所述步骤 A 中 LAC－PDU 数据分组头中的第一局域序列号时间标记也可以用底层传输序号代替，再建立 TCP 数据分组的序列号与该底层传输序号间的对应关系；所述步骤 B 中的第二局域序列号时间标记是终端成功接收的最大底层传输序号。

本发明的一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于：是用于移动通信系统传送数据分组的方法，该系统接收来自国际互联网的包含序列号的数据分组，并将该分组发往移动终端，所述的传送方法包括如下步骤：

接收来自国际互联网的数据分组；

将第一局域序列号时间标记赋予每个接收到的数据分组；

按移动通信系统使用的格式形成带有第一局域序列号时间标记的分组数据；

存储该带有时间标记的分组数据；

将所形成的分组数据发送到移动终端；

当移动终端成功地接收到所发送的分组数据时，移动终端回发确认数据，该确认数据包括确认序号和相应于所接收的第一局域序列号时间标记的第二局域序列号时间标记；

通过将存储的序列号和第一序列号时间标记与发回的确认数据进行比较，确定应向移动终端重传的数据分组；

重传所确定的数据分组。

所述的传送数据分组的方法中，所述的移动通信系统包括一个服务器，所述的服务器将第一局域序列号时间标记赋予每个接收到的数据分组，并按移动通信系统使用的格式形成带有第一局域序列号时间标记的分组数据，和存储该带有时间标记的分组数据。

本发明的一种将 TCP 用于不可靠传输网络的局域重传方法，其特征在于：是接收移动通信系统中移动终端数据分组的方法，该系统接收来自国际互联网的包含序列号的数据分组，并将该分组发往移动终端；所述的接收方法包括以

下步骤:

接收一个新的数据分组，该数据分组按移动通信系统使用的格式形成，所形成的数据分组包括第一局域序列号时间标记;

相应于所接收到的第一局域序列号时间标记给出第二局域序列号时间标记;

回发确认数据，该确认数据包括确认序列号和相应于所接收到的第一局域序列号时间标记给定的第二局域序列号时间标记。

本发明方法的适用环境是针对客户终端如移动终端，通过不可靠传输链路如无线传输链路，接入数据网络如国际互联网络，所建立的从远端服务器到无线接入点服务器到移动终端的单向 TCP 连接。本发明方法对在不可靠传输链路接入中，乱序的 TCP 数据分组的非拥塞丢失问题，采用了用第一局域序列号时间标记来标识 TCP 数据分组在不可靠传输链路这一段上的实际发送的先后顺序，然后根据含有 TCP 的确认分组（ACK1）中的确认序号（AN）以及相应的第一、第二局域序列号时间标记，判断与确认序号（AN）相对应的数据分组是否发生丢失，若发生丢失，则重传丢失的数据分组，即进行局域重传，并通过明晰重传（ERN）反馈来防止 TCP 源端发生窗口误动作。因此，本发明的方法是一种局域序列号时间标记与确认序号（AN）联合判断数据分组丢失及明晰重传反馈的方法。

本发明方法的有益效果是: 由于利用了 TCP 的确认分组（ACK1）与局域序列号时间标记（time-stamp）联合判断数据分组丢失并进行局域重传，因而不需要低层额外的控制开销，就实现了非拥塞丢失数据分组的即时重传恢复，具有恢复速度快、效率高的特点，并且可以对乱序传送的 TCP 数据分组丢失进行有效的恢复。

下面结合实施例及附图进一步说明本发明的方法。

图 1 是包含无线接入的混合网络中单向 TCP 连接的结构示意图。

图 2 是无线接入点向移动终端发送的数据分组的结构示意图。

图 3 是数据分组的 TCP 序列号与第一局域序列号时间标记的对应示意图。

图 4 是通过确认分组（ACK1）判断数据分组丢失的方法流程框图。

参见图 1，图中示出一具有无线接入的混合网络，如基于 IMT2000 的移动通信系统，10 是国际互联网络（因特网），20 是国际互联网络 10 的某一源端服务器，即 TCP 源端，30 是某一无线（不可靠链路）接入点服务器，40 是某一移动终端（也可以是移动计算机、用户终端或用户计算机）。无线接入服务器位于移动通信系统中，该系统包括移动交换机、无线网络控制器和基站，无线接入服务器可建立在移动交换机、无线网络控制器或基站中，进而可不建无线接入服务器，而将其功能安装到移动交换机、无线网络控制器或基站中。

无线接入点服务器 30 的操作过程是：从国际互联网络 10 上每接收到一个由 TCP 源端 20 发出的新的 TCP 数据分组，就将它封装在一个链路接入控制－协议数据单元（ＬＡＣ－ＰＤＵ，Link Access Control-Protocol Data Units）中，每个链路接入控制－协议数据单元（ＬＡＣ－ＰＤＵ）的数据分组的ＬＡＣ－ＰＤＵ分组头中含有一个固定比特长度的域，用于记录实际发送的序列号即发送顺序，称第一局域序列号时间标记（time-stamp）。该数据分组的ＬＡＣ－ＰＤＵ的结构可结合参见图 2，为“含有第一局域序列号时间标记（time-stamp）的“LAC-PDU 头＋IP 头+TCP 头+数据 DATA”。在ＬＡＣ－ＰＤＵ分组头中填入第一局域序列号时间标记的同时，还将该 LAC－PDU 数据分组的副本存入（复制）缓冲器中。

随着发送数据分组数的增加，该第一局域序列号时间标记（time-stamp）的值也从零开始以步长为 1 不断增加，如此，每个 TCP 数据分组在从无线接入点服务器 30 到移动终端 40 的整个发送过程中的实际发送顺序，就可以由该 LAC－PDU 数据分组中对应的第一局域序列号时间标记（time-stamp）值唯一确定。如图 3 中所示，＃1、＃2、＃4、＃3------表示各ＴＣＰ数据分组的序列号，0、1、2、3------（基准为 0）表示各 LAC－PDU 数据分组＃1、＃2、＃4、＃3------中对应的第一局域序列号时间标记（time-stamp）值，沿时间轴 t 顺序发送。

在国际互联网（如因特网）或大型局域网（如 WAN: 广域网）中，有很多连接数据源端和终端、实现可靠网络的通路。就是说若首先建立的通路发生网络拥塞，该系统可选择其它通路去传送数据，但不同的通路传送时间不同，所以在数据传送期间，通路变更会引起数据传送的失序，如无线接入服务器按＃1、＃2、＃4、＃3------的顺序接收 TCP 分组数据就是一个案例。

移动终端 40 对每个成功发送（接收）的ＴＣＰ数据分组都会产生一个确认分组（ACK1），该确认分组（ACK1）与 TCP 数据分组一样也封装在一个 LAC-PDU 中，在该 LAC-PDU 的分组头中含有记录第二局域序列号时间标记（time-stamp）的域，所记录的是当前移动终端 40 已经接收的由成功传送的各 TCP 数据分组所携带的第一局域序列号时间标记（time-stamp）中的最大值，当前移动终端将该含有第二局域序列号时间标记（time-stamp）及确认的数据分组序列号 AN（Acknowledge Number）的确认分组（ACK1）发送回无线接入点服务器 30，无线接入点服务器 30 根据接收到的确认分组（ACK1）所携带的第二局域序列号时间标记（time-stamp）、确认的数据分组序列号（AN）和与该数据分组序列号（AN）对应的 TCP 数据分组的第一局域序列号时间标记，来判断是否有 TCP 数据分组在无线传输链路上丢失。其判断的方法可进一步结合参见图 4。所述的确认序列号是表示预期的下一个序列号，在回发时，它也表示连续接收到的上一个 TCP 数据分组的 TCP 序列号，它还表示连续接收到的上一个 TCP 分组数据加 1 的 TCP 序列号。

步骤 401，判断在无线接入点（基站）服务器 30 的缓冲器中是否有与确认分组（ACK1）中的确认的数据分组序列号 AN 相对应的 TCP 数据分组，若是，则执行步骤 402，若不是，则执行步骤 406；步骤 402，如果是，则取出该 TCP 数据分组中所携带的第一局域序列号时间标记（time-stamp），如为 ts；步骤 403，将 ts 与确认分组（ACK1）所携带的第二局域序列号时间标记（time-stamp），如为 ts_{max}，进行比较，判断 $ts < ts_{max}$，若该小于关系成立，则执行步骤 404、405、406，若该小于关系不成立，则直接执行步骤 406；步骤 404、

405，$ts < ts_{max}$ 关系成立，说明该与确认的数据分组序列号 AN 相对应的 TCP 数据分组已丢失，则更新其第一局域序列号时间标记（time-stamp）并重传该 TCP 数据分组，即用一个新的表示当前传送顺序的时间标记来更新与数据分组序列号 AN 相对应的 LAC－PDU 数据分组中的第一局域序列号时间标记，并重传该修正后的 LAC－PDU 数据分组；步骤 406，判断无线接入点服务器 30 的缓冲器中没有与确认分组（ACK1）中的确认的数据分组序列号 AN 相对应的 TCP 数据分组，或判断 $ts < ts_{max}$ 关系不成立，或在执行完步骤 404、405 后，则将无线接入点服务器 30 中所有序列号小于 AN 的所有 TCP 数据分组全部删除。

本发明方法，在确认分组（ACK1）头的备用比特（如有 6 个比特）中定义一位明晰重传ＥＲＮ反馈（或明晰重传通知）比特，当无线接入点服务器 30 的缓冲器中有与确认分组（ACK1）中确认的数据分组序列号 AN 相对应的 TCP 数据分组，则将此确认分组（ACK1）头的明晰重传（ＥＲＮ）反馈比特置为 1，并将含有明晰重传（ＥＲＮ）反馈比特及确认的数据分组序列号 AN 的确认分组（ACK1）发送到ＴＣＰ源端 20，ＴＣＰ源端 20 在收到明晰重传（ＥＲＮ）反馈比特为 1 的确认分组（ACK1）后，若与该确认分组（ACK1）相对应的 TCP 数据分组发生快速重传或超时重传时，不作任何减小发送窗口的操作，只是重发该ＴＣＰ数据分组。

第一或第二局域序列号时间标记（time-stamp）的值是固定的，其长度是一个无线接入点（基站）所能容纳的某一个ＴＣＰ连接的最大分组数，若每个ＴＣＰ数据分组长 576 字节，局域序列号时间标记（time-stamp）取值 0 至 127（一般来说，对于一个ＴＣＰ连接已足够），即可用 7 比特长的局域序列号时间标记（time-stamp）。

但，随着发送数据分组数的增加，当局域序列号时间标记（time-stamp）的值超过其所能表示的最大值时，则会发生溢出，将又会从零开始计数，这时的局域序列号时间标记（time-stamp）值将不能反映实际数据分组的序列号大小。因而，本发明还需要一个进位比特，该进位比特在发生溢出时取反，则在

步骤 403 时就可正确判断两个局域序列号时间标记（time-stamp）的大小关系。因此，建议还是用 8 比特长的局域序列号时间标记（time-stamp）为好。

本发明方法用局域序列号时间标记（time-stamp）来标识不可靠传输链路上ＴＣＰ数据分组的实际发送顺序，因此，只要能实现该功能，就可以采用其它任何等同的手段。

本发明实施例提出的是将 TCP 数据分组与局域序列号时间标记（time-stamp）一起封装在 LAC-PDU 中进行发送的方法，在许多已有的移动通信系统中，已提供了低层（链路层）的传输序号传递功能，就只需建立 TCP 数据分组的序列号与低层传输序号之间的对应关系，并且，移动终端将它们所接收到的最大的低层传输序号反馈给基站，也一样可以完成上述的丢失数据分组的判断功能，这里的低层传输序号实际起到了局域序列号时间标记（time-stamp）的作用。

本发明的方法，可以广泛应用于通过不可靠链路接入数据网络－因特网的多种可靠的数据通信方式中。

我们技术方案的关键思想是融合了ＴＣＰ与链路层的优点，以便降低链路层的额外开销，并且提供失序分组的有效可靠地传递。在我们的方案中，使用了可被看作ＴＣＰ段链路层顺序号码的时间标记（time-stamp），去表示在不可靠链路接入点的ＴＣＰ段的传输顺序。

通过模拟，我们的结论是：本发明方法的技术方案确可大大改善不可靠网络如无线网络的 TCP 性能。

00.08.18

说 明 书 附 图

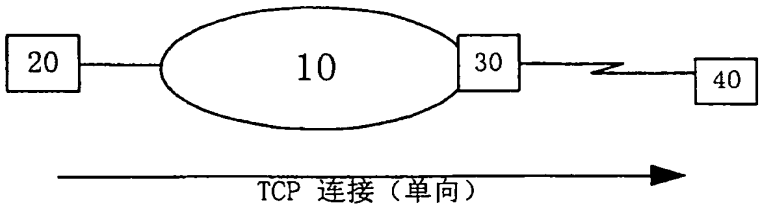


图 1

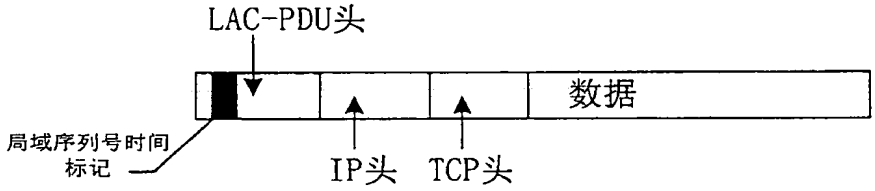


图 2

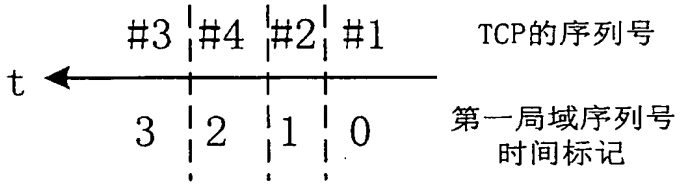


图 3

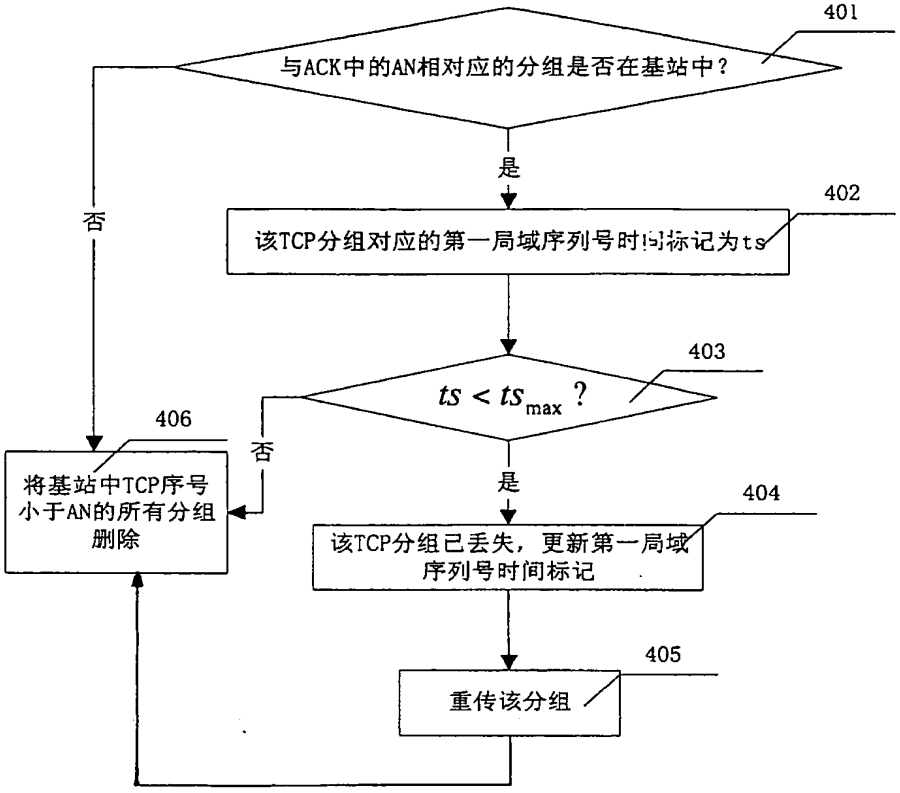

401
与ACK中的AN相对应的分组是否在基站中？
是
否
402
该TCP分组对应的第一局域序列号时间标记为ts
403
$ts < ts_{max}$?
否
是
406
将基站中TCP序号小于AN的所有分组删除
404
该TCP分组已丢失，更新第一局域序列号时间标记
405
重传该分组

图 4